УДК 004.[75+77]

ПРОБЛЕМЫ БЕЗОПАСНОСТИ SAAS

Дашко Д.А., Мешков В.И.
Государственный ВУЗ «Национальный горный университет», nmu.org.ua, dashkodo@gmail.com

В настоящее время, в эру унифицированного доступа к ресурсам заменой классических приложений являются SaaS решения. Если говорить о частных клиентах, то преимущество в виде доступа к приложению с помощью любых устройств (например drive.google.com) перевешивает все недостатки, в том числе недостаточную безопасность данных, но если говорить о корпоративных клиентах, то защищенность данных является одной из немногих значительных угроз для бизнеса. С этой точки зрения рынок SaaS решений не предоставляет требуемого уровня безопасности.

Ключевые слова – SaaS; безопасность; уязвимости SaaS, приложение как сервис.

ВВЕДЕНИЕ

В настоящее время безопасность является важнейшим вопросом при проектировании SaaS приложений, так как данные клиента всегда располагаются на удаленном, не контролируемом пользователями информационном ресурсе. Следует учитывать разницу между обычным веб-приложением и SaaS: концепция классического веб-приложения это доставка контента, в то время SaaS – это в первую очередь услуга. Предприятие (Клиент) не приобретает лицензию на пользование каким либо программным продуктом, не спонсирует разработку программного обеспечения для решения своей задачи, а использует готовое, доступное другим пользователям решение, предоставляемое удаленно.

ПРИМЕРЫ SAAS РЕШЕНИЙ НА УКРАИНЕ

К сожалению самостоятельные SaaS проекты только развиваются на территории Украины. К этим проектам можно отнести Yaware (система учета рабочего времени сотрудников), oki-toki.net (call-центр которые организовывается для клиентов на основе SaaS решения). Большая часть SaaS решений на Украине предоставляют сторонние SaaS продукты на основе собственных облачных ресурсов обработки данных, так например saas.com.ua предоставляет доступ к SaaS продуктам Microsoft (Dynamics CRM, Exchange, Sharepoint) на основе своих вычислительных ресурсов.

АРХИТЕКТУРА SAAS

SaaS подразумевает использование мультиарендной архитектуры, для которой необходимо наличие единой программной среды и общего аппаратного решения для всех клиентов для обеспечения максимальной эффективности использования ресурсов. В ряде случаев провайдер SaaS может предоставлять возможность использования собственной базы данных, благодаря чему повышается подконтрольность данных, хотя обычно используется SaaS на базе облачных хранилищ и вычислительных мощностей, тем самым обеспечивается распределенные хранение и обработка данных.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ SAAS РЕШЕНИЙ

Если говорить о безопасности то сюда стоит включать полную «цепочку» защиты, начиная от физической безопасности в дата-центрах, защищенных соединений и заканчивая аудитом бизнеса клиента для выявления уязвимостей. Аутентификация, активный аудит и шифрование должны стать частью дизайна SaaS для того, чтобы ограничить доступ к частной и конфиденциальной информации. SaaS провайдеры должны взять на себя ответственность за расходы и убытки, связанные с любыми данными нарушениями.

Существующие проблемы безопасности SaaS:

- SaaS не всегда предполагает использование облачных решений как платформы для хостинга приложений и, как следствие, не обеспечивается характерная для облачного хранилища репликация данных.
- Отсутствие стандартизации систем безопасности SaaS. Не все веб-сервисы и SaaS провайдеры прошли сертификацию по стандарту ISO27001.
- Выполнение SaaS приложения под правами администратора может привести к несанкционированному доступу к ресурсам SaaS провайдера.
- Проблема конфиденциальности данных лежит только на разработчике SaaS. Предлагаемая разработчиком модель защиты данных должна быть доступна всем, а защита данных должна зависеть только от реализованных мер защиты, а не от конфиденциальности описания системы защиты.
- Доступ из любой точки мира при наличии интернета наряду с удобством подвергает SaaS риску несанкционированного доступа к сервису.
- Отсутствие информации о том, где находятся наши данные. В некоторых странах есть нормативные акты регулирующих вытекание потоков данных за пределы страны, например Federal Information Security Management Act, который действует на территории США и запрещает частным организациям хранить конфиденциальные данные за пределами страны.

МЕРЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ SAAS

Таким образом, следует выделить основные меры защиты, которые могут быть внедрены в рамках SaaS:

- Сертификация в соответствие с международными стандартами информационной безопасности, на данный момент это стандарт ISO 27001.
- Разрешение доступа к SaaS только из доверенных узлов.
- Согласование деятельности и структуры SaaS в соответствие законодательным нормам пользователей SaaS.
- Использование брандмауэров и VLAN по мере необходимости.
- IDS – системы (системы обнаружения вторжения).
- IPS – системы (системы предотвращения вторжений).
- Тщательное логгирование всех видов деятельности, начиная с деятельности маршрутизаторов, межсетевых экранов, IDS, IPS, базы данных и заканчивая кодом приложения.
- Сервер для хранения логов должен быть независим от оборудования, на котором развернуто SaaS.
- Актуальные обновления антивируса на каждом сервере.
- Надежные пароли.
- Каждый пользователь должен иметь уникальный логин. Не должно быть никакого объединения с существующими учетными записями (OAuth).
- SaaS приложение не должно быть запущено под учетной записью администратора.

Несмотря на все еще не стандартизированные подходы к защите конфиденциальных данных в SaaS, сервисы набирают популярность благодаря своим неоспоримым преимуществам: сравнительно низкой стоимости владения и быстротой развертывания для предприятия. Реализация хотя бы выше отмеченных мероприятий повысит безопасность использования SaaS.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Progress Software. SaaS security and privacy. White paper. (Электрон. ресурс) / Способ доступа: URL: http://www.progress.com/docs/whitepapers/public/SaaS/SaaS-Security.pdf.

2. Колесов А. В преддверии SaaS (Часть 1) (Электрон. ресурс) / Способ доступа: URL: http://saasworld.ru/phparticles/show_news_one.php?n_id=354 – В преддверии SaaS (Часть 1)

3. Drew Robb. SaaS and Security: Is Your Data Safe? (Электрон. ресурс) / Способ доступа: URL: http://www.esecurityplanet.com/prevention/article.php/3743216/SaaS-and-Security-Is-Your-Data-Safe.htm – SaaS and Security: Is Your Data Safe